New Approach of Data Encryption Standard Algorithm

Shah Kruti R., Bhavika Gambhava

Abstract*—The principal goal guiding the design of any encryption algorithm must be security against unauthorized attacks. Within the last decade, there has been a vast increase in the accumulation and communication of digital computer data in both the private and public sectors. Much of this information has a significant value, either directly or indirectly, which requires protection. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. Performance and security level is the main characteristics that differentiate one encryption algorithm from another. Here introduces a new method to enhance the performance of the Data Encryption Standard (DES) algorithm is introduced here. This is done by replacing the predefined XOR operation applied during the 16 round of the standard algorithm by a new operation depends on using two keys, each key consists of a combination of 4 states (0, 1, 2, 3) instead of the ordinary 2 state key (0, 1). This replacement adds a new level of protection strength and more robustness against breaking methods.

Keywords- DES,Encryption,Decryption

I. INTRODUCTION

Cryptography is usually referred to as "the study of secret", while now a days is most attached to the definition of encryption. Encryption is the process of converting plain text "unhidded" to a cryptic text "hidded" to secure it against data thieves. This process has another part where cryptic text needs to be decrypted on the other end to be understood in figure 1.

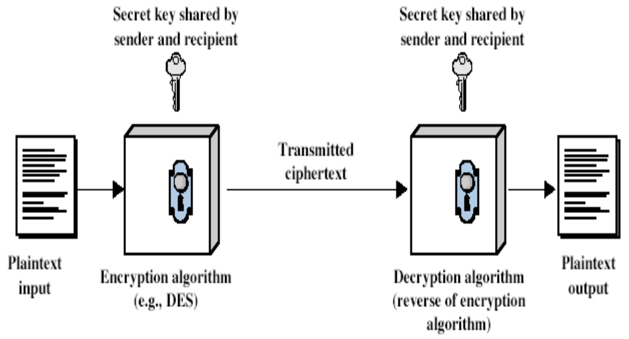

Figure 1. Encryption/Decryption

Cryptography Goals :[2]

1.CONFIDENTIALLY : Information in computer transmitted information is accessible only for reading by authorized parties.

2.AUTHENTICATION- Origin of message is correctly identified with an assurance that identity is not false.

3. INTERGRITY- Only authorized parties are able to modify transmitted or stored information.

4. NON REPUDIATION- Requires that neither the sender, nor the receiver of message be able to deny the transmission.

5. ACCESS CONTROL- Requires access may be controlled by or for the target system.

6. AVAILIBILITY- Computer system assets are available to authorized parties when needed.

II. DATA ENCRYPTION STANDARD

Without doubt the first and the most significant modern symmetric encryption algorithm is that contained in the Data Encryption Standard (DES).The DES was published by the United States' National Bureau of Standards in January 1977 as an algorithm to be used for unclassified data (information not concerned with national security). The Data Encryption Standard (DES), as specified in FIPS Publication 46-3, is a block cipher operating on 64-bit data blocks. The encryption transformation depends on a 56-bit secret key and consists of sixteen Feistel iterations surrounded by two permutation layers: an initial bit permutation *IP* at the input, and its inverse IP^{-1} at the output. The structure of the cipher is depicted in Figure 2. The decryption process is the same as the encryption, except for the order of the round keys used in the Feistel iterations.[12]

The 16-round Feistel network, which constitutes the cryptographic core of DES, splits the 64- bit data blocks into two 32-bit words, LBlock and RBlock (denoted by $L0$ and $R0$). In each iteration (or round), the second word Ri is fed to a function $\boldsymbol{f}$ and the result is added to the first word Li. Then both words are swapped and the algorithm proceeds to the next iteration. The function f of DES algorithm is key dependent and consists of 4 stages.

Manuscript received February 09, 2012.

Shah Kruti R.,Computer Engineerting Department, student of M.Tech(Computer Engineering) at Dharmsinh Desai University, Nadiad and Assistant Professor at Sardar Vallabhbhai Patel Institute of Technology, Vasad India, 9825590589., (e-mail: kruti13shah@gamil.com).

Bhavika Gambhava, Computer Engineerting Department, Dharmsinh Desai University, Nadiad, India, (e-mail: Bhavika.ce@ddu.ac.in).

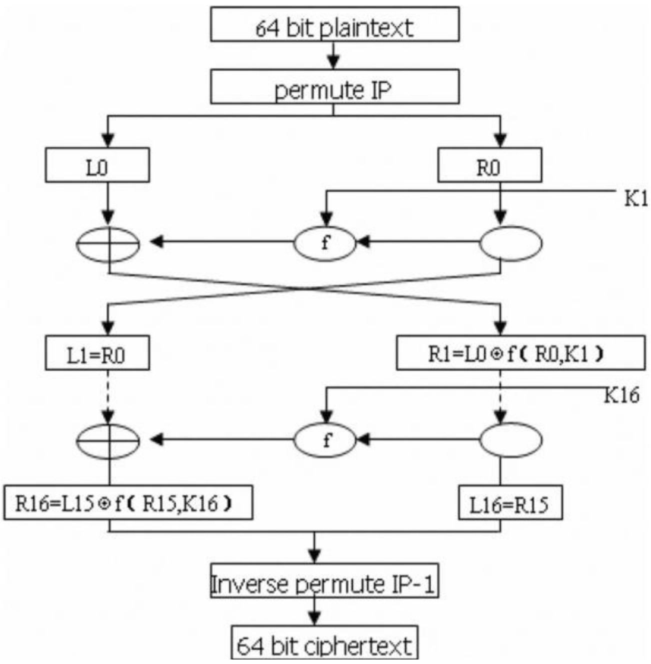

Figure 2.DES Algorithm

1. Expansion (*E*):The 32-bit input word is first expanded to 48 bits by duplicating and reordering half of the bits.[11]

2. Key mixing : The expanded word is XORed with a round key constructed by selecting 48 bits from the 56-bit secret key, a different selection is used in each round.

3. Substitution. The 48-bit result is split into eight 6-bit words which are substituted in eight parallel 6×4-bit S-boxes. All eight S-boxes, are different but have the same special structure.

4. Permutation (P) : The resulting 32 bits are reordered according to a fixed permutation before being sent to the output.

The modified RBlock is then XORED with LBlock and the resultant fed to the next RBlock register.The unmodified RBlock is fed to the next LBlock register. With another 56 bit derivative of the 64 bit key, the same process is repeated.

Pseudo Code : Data Encryption Standard

INPUT : plaintext m1 . . . m64; 64-bit key K=k1 . . . k64 (includes 8 parity bits).

OUTPUT : 64-bit ciphertext block C=c1 . . .c64.

1. (key schedule) Compute sixteen 48-bit round keys Ki, from K.

2. (L0, R0) ← IP(m1, m2,. . .m64) (Use IP Table to permute bits; split the result into left and right 32-bit halves L0=m58m50 . . . m8,R0=m57m49 . . . m7)

3. (16 rounds) for i from 1 to 16, compute Li and Ri as follows:

3.1. Li=Ri-1

3.2. Ri = Li-1 XOR *f* (R i-1, Ki)

where *f*(Ri-1, Ki) = P(S(E(Ri-1) XOR Ki)), computed as follows:

(a) Expand Ri-1 = r1r2 . . . r32 from 32 to 48 bits, T ←E(Ri-1).

(b) T ' ←T XOR Ki. Represent T ' as eight 6-bit character strings: T '= (B1 . . . B8)

(c)T " ←(S1(B1), S2(B2), . . . S8(B8)). Here Si(Bi) maps to the 4-bit entry in row r and column c of Si

(d)T''' ←P(T"). (Use P per table to permute the 32 bits of T"=t1t2 . . . t32, yielding t16t7 . . . t25.)

4. b1b2 . . . b64 ← (R16, L16). (Exchange final blocks L16, R16.)

5. C ← IP-1 (b1b2 . . . b64).

6. End.

Algorithm 1. DES Algorithm

III. IMPROVED 4-STATES OPERATION

To increase the security and key space, that makes the encryption algorithms more robustness to the intruders, a new manipulation bits process has been added in by using different truth table for manipulation bits process work on 4-states (0,1,2,3) , while the traditional binary process (XOR) work on (0, 1) bits only. The symbol # has been used to refer to the operator that execute this process use truth tables that shown in figure 3.[7]

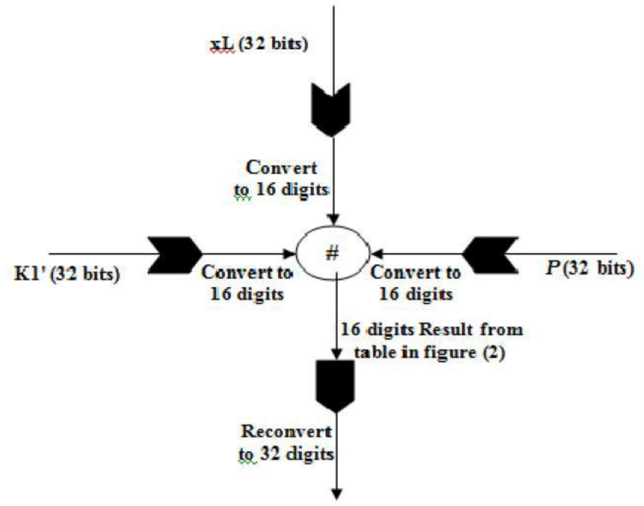

Figure 3.Design of Modified DES Algorithm

The new operation needs 3 inputs, the first one specify the table number that should be used to calculate the result among the 4 tables, the other 2 inputs define the row and column number in the specified table where the cross point of them gives the result.

Here, example for # operation, this operation need 3 inputs, first one specify the table number that should be used to calculate the result among the four truth tables as shown in Table 1, the other 2 inputs define the row and column number in the specified table where the cross point of them gives the result this result is in 16 digits.

Input in 32 bit binary format 10010111010100101010011110100010 01 which is converted into the number

2 1 1 3 1 1 0 2 2 2 1 3 2 2 0 2 1

Input 1: 0 1 3 0 1 2 2 3 1

Input 2: 3 2 2 1 0 1 2 1 1

Input 3: 1 0 0 2 1 3 2 1 2

Result : 3 0 2 3 1 2 2 2 2

#0	0	1	2	3
0	3	2	1	0
1	2	3	0	1
2	1	0	3	2
3	0	1	2	3

#1	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

#2	0	1	2	3
0	2	3	0	1
1	3	2	1	0
2	0	1	2	3
3	1	0	3	2

#3	0	1	2	3
0	1	0	3	2
1	0	1	2	3
2	3	2	1	0
3	2	3	0	1

Table 1.Truth Table

IV. PROPOSED ALGORITHM OF DES

This research proposed a new improvement to the DES algorithm. The proposed improvement makes use of the new operation defined in the previous section, operation (#) applied during each round in the original DES algorithm, where another key is needed to apply this operation, this key may come in binary form and convert to a 4-states key. Here, originally DES algorithm linear cryptanalysis and differential cryptanalysis attacks are heavily depends on the S-box design.

Consequently, multiple keys will be used in each round of the original DES, the first key Ki will be used with the ***f*** function. The second key will be the first input to the # operation, the second input will be the output of the ***f*** function, and the third input to the # operation will be the value Li, Algorithm shows the three 32-bits input to the # operation ,and the 32-bits output, with places needed to convert these 32- bits to 16-digits. These three inputs to the # operation should be firstly converted from 32 bits to a 16 digits each may be one of four states (0,1,2, 3), i.e., each two bits converted to its equivalent decimal digits.

Algorithm of modified data encryption standard with 4 state operation :

INPUT : plaintext m1 . . . m64; 64-bit two keys K=k1 . . . k64 and K'=k1' . . . k64' (includes 8 parity bits).
OUTPUT : 64-bit ciphertext block C=c1 . . .c64.
1. (key schedule) Compute sixteen 48-bit round keys Ki, from K.
 1.1. (key schedule) compute sixteen 32-bit round keys Ki', from K'
2. (L0, R0) ← IP (m1, m2,. . .m64) (Use IP Table to permute bits; split the result into left and right 32-bit halves L0=m58m50 . . . m8,R0=m57m49 . . . m7)
3. (16 rounds) for i from 1 to 16, compute Li and Ri as follows:
 3.1. Li=Ri-1
 3.2. Ri = Li-1 # *f* (R i-1, Ki)
where *f*(Ri-1, Ki) = P(S(E(Ri-1) Å Ki)), computed as follows:
 (a) Expand Ri-1 = r1r2 . . . r32 from 32 to 48 bits T ← E(Ri-1). (Thus T= r32r1r2 . . . r32r1.)
 (b) T' ← T XOR Ki . Represent T ' as eight 6-bit character strings: T ' = (B1 . . . B8)
 (c)T '' ← F where Function F = ((((((((S1+S2) mod 2 ^ 32) XOR S3) + S4) mod 2^32) XOR S5) +S6)mod 2^32
Here, Si(Bi) maps to the 8 bit entry in row r and column c of Si
 (d)T''' ← P(T''). (Use P per table to permute the 32 bits of T''=t1t2 .. ... …. t32,yielding t16t7 . . . t25.) and the operation # in Ri = Li-1 # *f* (R i-1, Ki) is computed as follows:
 (I)Convert the 32 bits resulted from *f* (R i-1, Ki) into 4-states 16 digits call it ***f* '**
 (II) Convert the 32 bits of Li-1 to 4-states 16 digits call it Li-1'
 (III) Convert the 32 bits of Ki' to 4-states 16 digits call it Ki''
 (IV) Compute Ri by applying the # operation on *f* ', Li-1', and Ki'' according to truth tables shown in Table.
4. b1b2 . . . b64 ← (R16, L16).
 (Exchange final blocks L16, R16.)
5. C ← IP-1 (b1b2 . . . b64). (Transpose using IP-1 C = b40b8 . . . b25.)
6. End.

Algorithm 2 Modified DES Algorithm

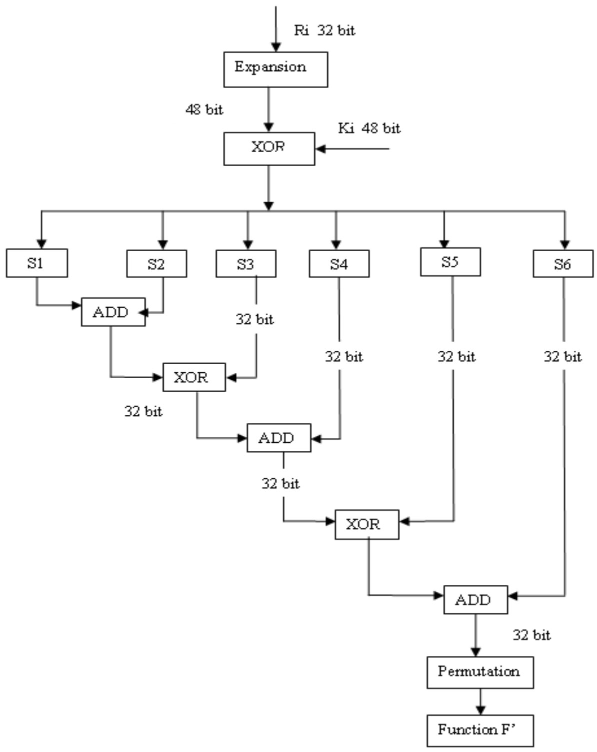

Figure 4.Function F Design

Here, using this proposed algorithm solve example .Our Input Message is 0123456789ABCDEF which is our plain text is converting into cipher text using this proposed algorithm. Here, There are 16 rounds for convert plain text to cipher text . In each round it contain two keys ,conversion of 16 bit data to 32 bit data and vice versa.

First we convert plain text into binary format also we have to convert key into binary format which is also in hex format. Now, performing all

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

operation of this proposed algorithm and get the cipher text. Function F we have to given 8 bit input using that input we got 32 bit o/p from the s-box and perform XOR operation and ADD operation.

Step1: Create Subkeys:K1 to K16
Key =133457799BBCDFF1
Step2 :Initial Permutation of Message which is given by User.
Step3 : for i =1 to 16 round
Ln = Rn-1
Rn = Ln-1 # f(Rn-1,Kn)
Step4: Convert 16 bit data into 32 bit data.

After complete one round we got
F' = 11 33 22 03 01 03 33 02
L' = 30 30 00 00 30 30 33 33
K' = 31 12 12 13 20 21 13 20
R1= 31 01 20 02 12 13 01 12
Here,R1 value found using truth table and got 16 bit data that is converted into 32 bit data.
R1 = 1101 0001 1000 0010 0110 0111 0001 0110
After completing all 16 round we got L16R16 value.
L16 : 0000 1011 0011 0011 1110 1010 1001 0100
R16 : 1111 0010 0111 0000 0000 0110 1111 0100

R16 L16 = 1111 0010 0111 0000 0000 0110 1111 0100 0000 1011 0011 0011 1110 1010 1001 0100
Now, Inverse of IP has been performed :
IP^{-1} : 1010 0000 1110 1100 0000 0111 1000 1000 0111 0001 0111 1001 0101 101 0100 1011

So, finally we got our cipher text **A0EC07887178594B**
Now, compare this solution with our original des algorithm we got avalanche effect and also solve cryptanalysis attack.

V. CONCLUSION

As we toward a society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique. DES is now considered to be insecure for some applications like banking system. there are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable. By adding additional key, modified S-Box design, modifies function implementation and replacing the old XOR by a new operation as proposed by this thesis to give more robustness to DES algorithm and make it stronger against any kind of intruding. DES Encryption with two keys instead of one key already will increase the efficiency of cryptography.

ACKNOWLEDGMENT

I take this opportunity to acknowledge those who have been great support and inspiration through the research work. My sincere thanks to Prof. Bhavika Gambhava for her diligence, guidance, encouragement and help throughout the period of research, which have enabled me to complete the research work in time. I express my deep sense of gratitude to Prof. C. K. Bhensdadia, Professor and Head of Computer Engineering Department of Dharmsinh Desai University, Nadiad, Gujarat for providing the necessary facilities during the research and encouragement from time to time. I also thank him for the time that he spread for me, from his extreme busy schedule. Special thanks to the institute, Dharmsinh Desai University, for giving me such a nice opportunity to work in the great environment. Thanks to my friend and colleague who have been a source of inspiration and motivation that helped to me during my dissertation period. And to all other people who directly or indirectly supported and help me to fulfill my task. Finally, I heartily appreciate my family members for their motivation, love and support in my goal.

REFERENCES

1. National Bureau of Standards – Data Encryption Standard, Fips Publication 46,1977.
2. O.P. Verma, Ritu Agarwal, Dhiraj Dafouti,Shobha Tyagi " Performance Analysis Of Data Encryption Algorithms " , 2011
3. Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha " Performance Evaluation of Symmetric Cryptography Algorithms, IJECT, 2011.
4. Diaa Salama, Abdul Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhound " Performance Evaluation of Symmetric Encryption Algorithm ", IJCSNS, 2008
5. Dr. Mohammed M. Alani " Improved DES Security" ,International Multi-Conference On System, Signals and Devices, 2010
6. Tingyuan Nie, Teng Zhang " A Study of DES and Blowfish Encryption Algorithm",TENCON, 2009
7. Afaf M. Ali Al- Neaimi, Rehab F. Hassan " New Approach for Modified Blowfish Algorithm Using 4 – States Keys" , The 5th International Conference On Information Technology,2011
8. J.Orlin Grabbe "The DES Algorithm Illustrated"
9. Dhanraj, C.Nandini, and Mohd Tajuddin " An Enhanced Approch for Secret Key Algorithm based on Data Encryption Standard", International Journal of Research And Review in Computer Science, August 2011
10. Gurjeevan Singh, Ashwani Kumar, K.S. Sandha "A Study of New Trends in Blowfish Algorithm ", International Journal of Engineering Research and Application,2011
11. W. Stallings, Cryptography and Network Security: Principles and Practices, 5th ed., Prentice Hall, 1999.
12. B.Scheier, Applied Cryptography : Protocols, Algorithms and Source Code in C,2nd ed.., John Wiley & Sons, 19995.

AUTHOR PROFILE

Kruti R. Shah is a student of Master of Technology in Computer Engineering at Dharmsinh Desai University, Nadiad, Gujarat, India. She is also an Assitant Professor at Saradar Vallabhbhai Patel Institute of Technology, Vasad, Anand, Gujarat, India. She has received her B.E degree from S'AD Vidya Mandal Institute of Technology, Bharuch, Gujarat, India in 2009. She has joined M.Tech at Dharmsinh Desai University, Nadiad, Gujarat, India in 2010.Her Current research interest is Information Security.

Bhavika Gambhava is Assistant Professor at Department of Computer Engineering , Faculty of Technology, Dharmsinh Desai University, Nadiad, Gujarat, India. She has received her B.E degree from L.D College of Engineering, Ahmedabad, Gujarat, India in 2004. She has received her M.E degree from Dharmsinh Desai University, Nadiad ,Gujarat, India.